Elsevier
LexisNexis
Reed Exhibitions
Reed Business

January 28, 2011

Via Email: privacynoi2010@ntia.doc.gov

Secretary Gary Locke
Office of Policy Analysis and Development
National Telecommunications and Information Admin.
U.S. Department of Commerce
1401 Constitution Avenue, NW, Room 4725
Washington, DC 20230

RE: Comments on "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework"

Dear Secretary Locke:

Reed Elsevier Inc. ("Reed Elsevier") appreciates this opportunity to provide comments in response to the request for public comment by the Department of Commerce ("DoC" or "Department") regarding the framework for consumer privacy proposed in its December 2010 Internet Policy Task Force Report, "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework (the "Report").

We commend the Internet Policy Task Force for relying heavily on the input of industry in preparing the Report. The Department's encouragement of industry self-regulation and its embrace of a multi-stakeholder approach with the government serving as the coordinator of this process is strongly supported by Reed Elsevier. This approach was at the forefront of the development of the commercial internet that began in the 1990s, and Reed Elsevier believes this approach should not be abandoned as we work on the complex commercial privacy issues discussed in the Report.

As the policy recommendations included in the Report are finalized, we urge the Department to recognize the important distinction between companies that collect information directly from consumers and those that do not. Reed Elsevier and similar information companies have few direct consumer relationships. Unlike companies that collect information directly from consumers, Reed Elsevier relies primarily on information from government agencies and third-party data sources. Further, most products and services offered by Reed Elsevier are designed for use by business, professional or government users. Non-consumer facing companies occupy a unique position in the information marketplace. As such, we have concerns with some of the key components outlined in the proposed framework that are unworkable where information is not

collected directly from consumers. We look forward to working with the Department to address these issues as the Report is finalized.

I. Introduction

Reed Elsevier is one of the world's leading publishing and information companies, providing professional information solutions in the business, risk, legal and scientific sectors. Elsevier is the world's leading publisher of science and health information, publishing over 2,000 journals and close to 20,000 books and major reference works in the scientific, technical and medical fields. Reed Business Information publishes over 400 business-to-business magazines, directories and newsletters and provides access to over 200 online communities. Reed Exhibitions is the world's foremost organizer of business-to-business trade shows, organizing over 440 events in 36 countries and attracting over 6 million event participants in 2009. LexisNexis is a leading provider of information products and services to the government, legal and corporate markets and serves over one million users daily.

All major Reed Elsevier businesses depend on the collection and use of information about persons. Medical and scientific journals published by Elsevier include information about authors and researchers and in some instances, anonymized information about selected patients or test subjects. Reed Business depends on information about persons in producing online and offline periodicals, including information about authors, interviewees and individuals in the news. Reed Exhibitions relies on access to business contact information to organize its business-to-business trade shows. LexisNexis depends on access to information to develop and update its many online and offline products including directories, news reports, court decisions and products used to help businesses and government manage risk through fraud detection and prevention, identity authentication, debt collection, and intelligent risk management and modeling.

LexisNexis products are used by businesses, non-profit organizations and government agencies for a host of important and socially beneficial purposes. Some examples of these uses are discussed below.

Our information products and services have been donated to the National Center for Missing and Exploited Children ("NCMEC") since 2001. These information products and services have been instrumental in helping NCMEC to locate individuals that may have abducted a missing child and have helped in the recovery of hundreds of missing children. NCMEC's ability to locate and recover missing children is dependent on access to accurate, up-to-date information.

Another innovative and important use of our products is combating sex crimes. LexisNexis helps law enforcement locate non-compliant sex offenders in order to keep our children and communities safe. LexisNexis sex offender solutions leverage content and technology to find both registered and unregistered sex offenders by street address and can map their proximity to schools, churches, day care centers, playgrounds and other areas where children congregate. Numerous state and local law enforcement agencies depend on information provided by LexisNexis in locating sex offenders who have violated registration requirements, or who may be involved in a child abduction or other offense.

LexisNexis offers numerous identity authentication and fraud detection products. Our ChargeBack Defender® product is used by merchants to prevent the use of stolen credit cards to purchase products online, over the telephone, and in other "card-not-present situations" where merchants cannot look at a credit card, check the signature, or check other identification. This product relies on data provided by consumers to merchants that is verified against data in our system to help determine whether the individual with whom the merchant is interacting is who that person purports to be. One of the largest personal computer manufactures in the country experienced a 70% reduction in annual fraud losses by using this product.

Another example of our authentication products is Instant ID® Q&A, which is used by merchants, credit card issuers and banks to help them authenticate consumers and detect and prevent identity theft and fraud. This product uses information from many sources to develop questions that can be used to help authenticate identity. For credit card transactions specifically, the product enables retailers to verify identity information provided by a consumer before making the decision to accept credit. After a top-five credit card issuer in the country began using Instant ID® Q&A, the issuer experienced a 10% reduction in annual fraud losses. This reduction in losses resulted in a net savings of more than $1 billion annually that benefited consumers by keeping down the cost of credit.

These identity confirmation and antifraud services provide tremendous benefits to consumers because our tools make it much harder for fraudsters to use stolen identities to defraud companies and financial institutions. The victims in such frauds are consumers whose identities are stolen. Fraudsters today use very sophisticated methods. With our services those organizations seeking to prevent identity theft also have access to sophisticated tools to defeat fraud attempts.

LexisNexis also offers a number of products that are used by insurance companies to detect fraudulent property and casualty insurance claims, reducing fraud losses and reducing rates charged to consumers. In addition, LexisNexis provides products used for employment, resident and volunteer screening. These products are used to prevent harm to employees and co-workers, customers and persons in custodial care. Employers use these products to implement cost-saving fraud prevention measures and avoid liability.

II. Fair Information Practice Principles (FIPPs)

Despite the diversity of Reed Elsevier's product offerings, they all share one thing in common—a reliance upon the collection, use and sharing of information in order to operate and continually improve. As such, Reed Elsevier strongly supports the Report's emphasis on balancing privacy protections with the free flow of information. Like the Department, Reed Elsevier seeks an approach that protects consumer privacy while continuing to encourage growth in the vibrant e-commerce sector of the economy. This continued upward trajectory depends in large part on maintaining consumer confidence in the sector. Commercial data privacy protection is crucial to encouraging these goals.

As discussed above, our products are used by businesses, non-profits and government agencies for a host of important and socially beneficial purposes. Although Reed Elsevier supports improving data security, many of the proposed restrictions on

the free flow of information would adversely impact our ability to provide our products and services to our customers and would negatively impact commerce.

Reed Elsevier acquires consumer data from a variety of resources, and except for a few limited instances does not interact directly with consumers. As such, proposals that require notices and disclosures to consumers impose challenging burdens on businesses such as Reed Elsevier that rely upon third party sources to build and maintain their information products.

For companies in this sector, certain of the Fair Information Practice Principles ("FIPPs") discussed in the Report do not work well. Unlike consumer-facing companies that collect information directly from individuals, information companies rely upon information from government agencies or third-party data sources. This makes many of the proposals within the framework, such as those requiring enhanced notice and choice to individual consumers and disclosure of purpose specifications to individuals, not workable for these types of companies. Further, requiring access and correction to databases used for fraud detection and law enforcement purposes can seriously undermine the integrity of these databases and put law-biding citizens at risk. Our specific concerns are discussed below.

A. Transparency

The Report favorably cites "enhanced transparency" as a way to improve the current notice-and-choice framework and provide consumers with clear information with which to make informed choices about their personal data.[1]

An enhanced notice that provides consumers with the choice to opt-out of Reed Elsevier's databases would be unworkable for us and for information companies like us. Many of our databases are used for fraud detection and prevention, identity authentication and law enforcement applications. Providing "choice" to individuals regarding their inclusion in these databases would severely weaken the effectiveness of these databases. Moreover, many of the records we obtain are public records which are public as a matter of law and do not require consent for collection.

It is critical for databases comprised of public records and other public documents to be complete and comprehensive. These records are used to trace events over time, such as the creation and conveyance of property titles or the development of law. In addition to short-term utility, these records are important documents of historical value and cannot be changed or omitted without harm to the entire collection.

Similarly, Reed Elsevier maintains databases of published news and business reports. News reports are prepared as notable events occur and are considered by many historians to be primary source materials for historic research. News reports are also protected speech under U.S. law and not subject to change or deletion except in very limited circumstances.

Reed Elsevier opposes any proposal to provide additional access and correction rights to consumers. Under the Fair Credit Reporting Act ("FCRA"), consumers are

[1] Report, p. 34.

already entitled to receive notice of the most important adverse actions that may involve the use of personal information, such as denials of employment, credit, insurance, or housing. The FCRA also provides the affected consumer with a copy of the information that the consumer reporting agency at issue maintains about such consumer. The FCRA also allows consumers to seek corrections to any data that is inaccurate or incomplete. Applying an access and correction requirement more broadly than in the FCRA context would impose burdensome compliance costs on a huge number of businesses, with little or no additional benefit to consumers.

The Report discusses the creation of privacy impact assessments, or PIAs, as a way for commercial entities to increase transparency about their data practices. Reed Elsevier strongly supports the concept of privacy by design, and we routinely consider privacy when developing our products. The purpose for which a product is developed drives decisions made about its design and privacy protections are a very important factor in this calculation. However, we do not support the creation of a formal PIA process for the private sector. Our current process for analyzing privacy concerns when creating new products is fluid and dynamic, matching our sometimes rapid timetables for product development. We also oppose any requirement that PIAs be published, potentially exposing proprietary business information and practices. By imposing a formal legislative requirement, we are concerned that an emphasis on form over substance will prevail when analyzing the privacy implications of new products.

B. Individual Participation

One component of individual participation, as described by the Report, would include seeking individual consent for the collection, use, dissemination, and maintenance of PII. Individual, affirmative consent does not work for non-consumer facing companies like Reed Elsevier that rely on information from public records and other third-party information sources. This requirement would severely undermine the effectiveness of our information products, as discussed below.

Information companies often purchase their data from third parties, and do not have any control over how purchased data is sourced by those third parties. It would not be possible to obtain affirmative consent from a sufficient number of individuals to maintain comprehensive information in our databases. Even if we could convince our third party data suppliers to provide disclosures and seek such affirmative consent, we know from historical data that the numbers of individuals who respond to an opt-in request will be extremely low.

In addition, Reed Elsevier opposes universal opt-out requirements. Because many Reed Elsevier databases are used for law enforcement, public safety, and anti-fraud purposes, allowing criminals and fraudsters the ability to opt-out of having their information included in databases would significantly diminish the effectiveness of such databases. As a result, the commercial, law enforcement, and nonprofit interests that rely on these databases would likely find the databases less effective, to the detriment of crime victims and consumers. For the same reason, an affirmative consent requirement would not work for these databases, since bad actors who do not wish to be included in these databases would simply refuse to provide affirmative consent.

Reed Elsevier is also concerned that an access and correction requirement could be misused by bad actors to gain access to databases in order to perpetrate fraud against consumers based on data obtained from those databases. No verification system can be made perfect. The imposition of an access obligation on databases that contain personal information can facilitate fraud and other criminal activity by allowing criminals to "game" the system. Fraudsters and criminals could exploit access rights to gather additional information for use in fraud schemes, such as "phishing" or other scams that use known information to induce consumers to reveal more compromising personal information.

Similarly, imposition of a correction requirement for data obtained from third parties, including data obtained from government agency records or from proprietary private sources such as journalistic reports and research articles, raises the possibility that consumers could seek changes to widely distributed versions of public records where the privately held version differs from the official record. Such a change could take the form of a change to the name of an owner on a property record or an alteration in the outcome of a court decision. Also, changes to news reports should be made only by the publisher and author, not by the distributor who does not legitimately control the content, notwithstanding the consumers' disagreement with the substance of the report.

As discussed previously, the FCRA requires that consumers receive notices for the most important adverse actions that may derive from the use of personal information, such as denials of employment, credit, insurance, or housing. The FCRA also provides the affected consumer with a copy of the information that was used in making the adverse decision and allows consumers to seek corrections to any data that is inaccurate or incomplete. Therefore, no additional access and correction requirements are necessary. Applying an access and correction right more broadly than is required in the FCRA context would impose burdensome compliance costs on businesses and negatively impact commerce, with little or no additional benefit to consumers.

Even a narrow access and correction requirement could have unintended consequences. Reed Elsevier's databases are used to support its multiple product offerings. Allowing access and correction for one or two purposes, such as identity authentication, may "poison" the data for other purposes, such as fraud detection and prevention or law enforcement. Information contained in a telephone directory may be used to help locate a material witness in a child abduction case. The right to "correct" the directory listing could be used to modify the address so as to misdirect anyone looking for the witness.

C. Purpose Specification

The Report seeks increased alignment between consumer expectations and actual information practices by focusing on purpose specification and use limitations, which would require organizations to disclose the specific reasons for which it collects information, and then limit the organizations to those purposes.[2]

Limiting the use of data to certain articulated purposes would negatively impact commerce and stifle innovation and new product development. Different companies

[2] Report, pp. 37-38.

can have many different business needs for the same data. Some of these needs may come from yet-to-be developed products. News reports or documents of historic significance, information with precedential value like court decisions, and official public records such as title records are retained without limit and for a number of different purposes. Their inclusion in our databases enhances the value of the databases by providing a complete historical record to researchers and interested parties. New uses for this data may emerge over time.

Data may be lawfully collected to support a broad range of unspecified activities. In a simple example, consider the multiple purposes for which individuals read a newspaper and how the same data may be used by an individual or by different individuals for varied, unrelated yet legitimate purposes. A news story about the health of a CEO could influence personal or commercial investments, business decisions, investment advice to third parties, personal medical treatment decisions by unrelated individuals, and for myriad other reasons. It is not possible for all of these uses to be identified in advance and included in a formal notice and it would be wrong either to prohibit unanticipated uses or to prohibit such uses by law while implicitly acknowledging and permitting such uses. Under the current legal regime in the U.S., data collection is lawful unless specifically prohibited. Information companies should not be required to specify the authority that permits the collection of different types of information.

Furthermore, multiple uses may be found for the same data and the uses for the same data may overlap. Removal of certain data when it is being used for one purpose would damage databases where the data is contained for another purpose. Prohibiting the use of previously collected historical data after the data has already been in the marketplace for some time would not serve the best interests of consumers or the business community. Such a prohibition will stifle innovation and hamper new product development, negatively impacting businesses and consumers.

D. Data Quality and Integrity

For information companies who procure data from third party sources and not from the consumer directly, verifying that the reported data matches the data provided by the consumer to the third party data source is not possible, since the information company and the consumer never liaise with one another. Data sourced from a government agency or court includes a presumption of accuracy notwithstanding conflicting claims that have not been resolved by the agency or court. Attempting to verify data through other means would impose costly and exceedingly burdensome requirements on information companies and would have a negative effect on businesses that depend upon information from third party sources.

A one-size-fits-all accuracy requirement would impose unnecessary costs on information companies and would adversely impact commerce. For example, it is not worth the cost and burden required to update a directory of contact information to standards of near-perfect accuracy, balancing how rapidly contact information changes versus the importance of accuracy in this type of information product. In other cases, where accuracy is more important, such as information used for FCRA-purposes, accuracy standards are already imposed by the FCRA.

Narrower propositions to verify the accuracy of information against the third party source from which it was acquired, i.e., to verify that the information was not inadvertently altered in any way post-acquisition, may be workable for information companies, but this proposition would have to be carefully vetted to ensure that it can be successfully implemented without imposing an excessive burden on information companies.

III. The Development of Voluntary Codes of Conduct

Reed Elsevier supports the Department's approach to privacy, and agrees that the development of voluntary, enforceable codes of conduct by industry are an appropriate means for addressing individual privacy without unfairly burdening the business community. Reed Elsevier believes that industry is best positioned to understand the challenges that they face on a daily basis as well as share a vision about what the future may hold for their industry. In this business environment characterized by ubiquitous data collection and rapid technological innovation, industry itself can create standards that are dynamic enough to adapt with the pace of change. Self-regulation is also very effective in protecting consumer privacy in global online media.

Although the Department and other government entities may have a hand in shaping the goals and standards of such a document (and the power to authorize recognition of a particular code as meeting the standards set by government), Reed Elsevier believes the government itself should not handle the creation of an industry code or dictate participation in a particular code. A "voluntary" code created by the government with mandatory participation would result in little more than legislation by another name, with all of the delay and lack of flexibility that can accompany legislation.

Reed Elsevier believes that this code must contain certain features in order to make it successful. First, it should include a safe harbor for businesses that adhere to the code, once it is in force. This provides an incentive for companies to agree to participate in the voluntary enforcement regime and to adhere to the standards of the code.

Second, the code must be enforceable by industry, but allow the government to step in and hold bad actors accountable if necessary. Law abiding corporate citizens have powerful incentives to police their own industry and punish bad actors who may be gaining an unfair advantage, and to promote policies that build consumer trust. There is no "fox guarding the hen house" in this scenario, because government will provide enforcement on the back end, and ultimately hold those businesses accountable for complying with the Code of Conduct they have agreed to abide by.

Reed Elsevier believes that industry codes are capable of handling both current and future privacy concerns in a way that is more flexible and nimble than what legislation and regulation can provide. Reed Elsevier also believes that the "Do Not Track" proposal being discussed by the Federal Trade Commission should not be codified into new legislation or regulations. A Do Not Track mechanism, if implemented broadly, could potentially prevent businesses from collecting information used in the development of new products and services. Moreover, the online advertising business is a highly dynamic market characterized by rapid technological change. In this environment, regulation that is specific to a technology or business model could deter

entry, thwart innovation, and limit competition in the sale of online advertising, as well as limit the products and services that consumers are accustomed to receiving for little or no cost because they are sponsored by advertising.

While we support uniform choice for consumers for online behavioral advertising, we believe that the government should not get involved in the development of a Do Not Track mechanism. At this time, significant self-regulatory efforts are underway that will provide uniform consumer choice for online behavioral advertising, as contemplated by the Federal Trade Commission, without sacrificing potential innovation in new products and services.

IV. Global Interoperability

Reed Elsevier supports the Department's continued efforts in the area of increased cooperation among global privacy enforcement authorities. We are especially interested in, and supportive of, acts by the Department to facilitate cross-border data transfers.

At the same time, Reed Elsevier believes that the United States' privacy framework provides the most flexible and nuanced approach to privacy protection in existence today. The explosion in innovation in e-commerce in this country and our status as the world's leader in internet technology and content makes this clear. While the legal regime regulating the internet can be improved and strengthened, it is important that we not do anything that will stifle innovation and adversely impact e-commerce. The Department should encourage other countries to follow our lead and adopt more flexible privacy frameworks that mimic the U.S. approach. Our framework provides consumer protection in areas where it is needed while, at the same time, providing enforcement authority against bad actors when required.

Reed Elsevier supports the Department's continued work with the APEC Data Privacy Pathfinder project, provided that the Department approaches this project as only one of many possible ways through which greater global interoperability can be obtained.

V. National Requirements for Security Breach Notification

Reed Elsevier supports a uniform, national security breach notification law with a strong state law preemption requirement. At the current time, almost all 50 states have breach notification laws, which has resulted in a frustrating and sometimes conflicting series of mandates and potential enforcement problems for companies that operate across state borders. Moreover, because of the comprehensive status of most of the information in our databases, many data breaches implicate multiple state laws. We welcome the clarity and uniformity that a single security breach notification statute would bring. It will not solve the problems of inconsistency, however, unless state breach notification laws are fully preempted, and states are prohibited from imposing varying obligations upon companies in the case of a multi-state breach. The following are key issues that should be considered in developing security breach notification legislation.

A national breach notification law should only apply to sensitive personally identifiable information. Those data elements should be limited to the following:

An individual's first and last name or first initial and last name in combination with:

- A non-truncated social security number; or
- A driver's license number, passport number, state identification card number, or alien registration number; or
- A financial account number or credit or debit card number in combination with any security code, access code, or password that is required for an individual to obtain credit, withdraw funds, or engage in a financial transaction.

The trigger for breach notification should be limited to those breaches where there is a significant risk of identity theft or financial fraud. This will help prevent over-notification of consumers and ensuring that the notice that consumers receive is meaningful.

Any federal security breach notification rule should also exclude public record and publicly available information. This information is generally available and widely used by consumers and businesses already. A requirement for a company to provide notice to consumers of a security breach when the only data accessed is public record or publicly available information does not make sense since this information is already in the public domain.

* * *

Reed Elsevier appreciates the opportunity to provide these comments to the Department. We commend the Internet Policy Task Force for relying heavily on the input of industry in preparing the Report. The Department's encouragement of industry self-regulation and its embrace of a multi-stakeholder approach with the government serving as the coordinator of this process is strongly supported by Reed Elsevier. It is important that any policy recommendations included in the final Report recognize the important distinction between companies that collect information directly from consumers and those that do not. Further, we urge the Department to carefully consider the impact that any proposed policy recommendations would have on the ability of companies to use information for fraud detection, prevention, and identity authentication purposes, and the impact such restrictions may have on commerce. Finally, we urge the Department not to propose an affirmative consent requirement for uses of data, including new uses of data, as this requirement would undermine both the development of new information products and the effectiveness of existing information products used by financial institutions, retailers and others in processing transactions.

Reed Elsevier thanks the Department for avoiding formal recommendation of a policy at this time and for recognizing that the Report represents only the beginning of policy discussions on these complex issues. The Department's commitment to the multi-stakeholder approach and its wariness of premature regulation is fully supported by Reed Elsevier. We thank the Department for its thoughtful approach. Given the importance of encouraging continued innovation in the e-commerce sector and the

rapidly evolving technologies involved, we look forward to working with the Department as it continues to develop this policy framework. If you have any questions, please call me or contact Steven Emmert, Senior Director, Government and Industry Affairs, at 202-857-8254.

Sincerely,

Steven Manzo
Vice President, Government Affairs
Reed Elsevier Inc.